The Vulnerability Window Is Shrinking

By Michael C. Maschke, Sharon D Nelson, Esq., and John W. Simek

For years, law firms have approached cybersecurity with a simple assumption: when a new vulnerability is discovered, there will be time to respond.

That assumption may be getting harder to defend.

Google recently disclosed that it disrupted a cyberattack in which threat actors allegedly used artificial intelligence (AI) to identify and exploit a previously unknown software vulnerability. The attack was stopped before it caused damage, but the implications extend well beyond a single incident.

The real story is not that AI is helping hackers. The real story is that AI accelerates the entire cybersecurity lifecycle. That means the vulnerability window, the time between discovery and exploitation, may be shrinking.

AI is Changing the Pace of Cybersecurity

Much of the public conversation about AI has focused on productivity gains, automation, and efficiency. Cybercriminals are pursuing the same benefits.

AI can help analyze code, identify weaknesses, automate reconnaissance, and accelerate research that once required significant manual effort. Technology is not replacing skilled attackers, but it can make them faster and more effective.

For organizations, this creates a simple challenge. If vulnerabilities can be discovered faster, they can potentially be exploited sooner as well.

Historically, organizations often had days, weeks, or even months to identify and remediate vulnerabilities before they were widely exploited. Although that timeline was never guaranteed, it provided some breathing room. As AI-assisted vulnerability discoveries become more common, that breathing room will continue to shrink.

Why Law Firms Should Care

Law firms remain attractive targets for cybercriminals because they hold some of the most valuable information in the business world, including privileged communications, litigation strategy, intellectual property, merger and acquisition documents, financial information, and sensitive client records.

At the same time, firms rely on increasingly complex technology ecosystems. Cloud platforms, document management systems, collaboration tools, client portals, practice management applications, and third-party vendors all expand the firm's digital footprint. The challenge is not simply protecting these systems. It is protecting them quickly enough.

When cybersecurity teams discover a critical vulnerability, every hour matters. Delays in patching, uncertainty about asset inventories, or slow vendor response times can create openings for attackers. In an environment where AI may accelerate exploitation, speed itself becomes a security control.

Patch Management is Now a Business Issue

Too often, vulnerability management is treated as a technical responsibility that belongs exclusively to the IT department. That mindset is increasingly outdated.

Questions about cybersecurity now intersect with client expectations, professional responsibilities, cyber insurance requirements, business continuity planning, and risk management.

Firm leadership should understand how quickly critical vulnerabilities are identified and remediated. They should know whether internet-facing systems are continuously monitored and how third-party vendors are evaluated. They should also understand whether incident response plans are regularly tested.

These are no longer purely technical questions. They are governance questions.

Clients increasingly expect their outside counsel to demonstrate mature cybersecurity practices. Regulators are paying closer attention to cybersecurity controls, and cyber insurers continue to scrutinize security programs during underwriting and renewal.

Firms that treat cybersecurity as a leadership issue rather than a technology issue will be better positioned to navigate these pressures.

The Clock is Running Faster

The good news is that defenders are using AI as well. Security teams are leveraging AI to improve threat detection, identify vulnerabilities, prioritize remediation, and accelerate incident response. Technology is not inherently an advantage for attackers. However, it raises the stakes for organizations that remain slow to adapt.

Law firms do not need to panic every time a new AI-related cybersecurity headline appears. Nor do they need to overhaul their entire security strategy because of a single incident.

They do, however, need to recognize that the pace of change in cybersecurity is accelerating.

The Google incident offers a glimpse of what may become increasingly common: a world in which vulnerabilities are discovered, analyzed, and weaponized more quickly than ever.

The vulnerability window is shrinking. The question for law firms is whether their security programs are moving fast enough to keep pace.

Michael C. Maschke *is the President and Chief Executive Officer of Sensei Enterprises, Inc. Mr. Maschke is an EnCase Certified Examiner (EnCE), a Certified Computer Examiner (CCE #744), an AccessData Certified Examiner (ACE), a Certified Ethical Hacker (CEH), and a Certified Information Systems Security Professional (CISSP). He is a frequent speaker on IT, cybersecurity, and digital forensics, and he has co-authored 14 books published by the American Bar Association. He can be reached at mmaschke@senseient.com.*

Sharon D. Nelson *is the co-founder of and consultant to Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association, and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA. snelson@senseient.com.*

John W. Simek *is the co-founder of and consultant to Sensei Enterprises, Inc. He holds multiple technical certifications and is a nationally known digital forensics expert. He is a co-author of 18 books published by the American Bar Association. jsimek@senseient.com.*